EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://oliver.click	Checks	9 pruebas
Dominio	oliver.click	Hallazgos	49 totales
Fecha	19 de junio de 2026 a las 14:26	Problemas	17 detectados

D

53/100

puntos de seguridad

RESUMEN EJECUTIVO

El analisis de ciberseguridad realizado al dominio oliver.click arroja una puntuacion de 53/100, lo que resulta en una nota calificada como D. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 genero una advertencia y 3 fallaron de forma critica. La ausencia de configuraciones basicas de seguridad en el servidor y la exposicion de versiones de software desactualizadas representan un riesgo significativo. Se concluye que el sitio es actualmente vulnerable y requiere intervencion inmediata para mitigar posibles vectores de ataque.

Resumen de Riesgos

0	6	7	4	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 60 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	CMS detectado: WordPress
Version CMS Expuesta	20	FALLO	WordPress 7.0 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 60 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  60 dias restantes (expira: 2026-08-18T21:56:27.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-20T20:56:30.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: cloudflare — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.4.21 — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 7.0
- INFO **Tecnologias detectadas**
  PHP/8.4.21

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 7.0 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 7.0 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (1851 bytes)
- INFO **Reglas robots.txt**
  10 Disallow, 2 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://oliver.click/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto

- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Redireccion HTTPS ausente: El servidor responde a traves de HTTP sin redirigir al usuario a una conexion cifrada, permitiendo la interceptacion de datos.
[HIGH] Content-Security-Policy (CSP) faltante: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyeccion de contenido malicioso.
[HIGH] X-Frame-Options faltante: El sitio no esta protegido contra clickjacking, lo que permite que sea cargado en marcos externos para engañar a los usuarios.
[HIGH] Strict-Transport-Security (HSTS) faltante: El navegador no es forzado a usar conexiones seguras, aumentando el riesgo de ataques de degradacion de protocolo.
[HIGH] Exposicion de version de WordPress (7.0): Se detecto publicamente la version del CMS, lo que permite a atacantes buscar vulnerabilidades especificas y exploits conocidos.
[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La presencia de un puerto de servicio alternativo abierto incrementa la superficie de ataque y puede exponer servicios no asegurados.
[MEDIUM] X-Content-Type-Options faltante: No se previene el MIME-type sniffing, lo que podria permitir que archivos cargados sean ejecutados como scripts.
[MEDIUM] Archivo /readme.html accesible: Este archivo revela informacion tecnica sobre la instalacion de WordPress que deberia ser privada.
[MEDIUM] Referrer-Policy y Permissions-Policy faltantes: Falta de control sobre la informacion de procedencia enviada y sobre el acceso a funciones del navegador como camara o microfono.
[LOW] Cabeceras de servidor expuestas: Se revela el uso de Cloudflare y la version exacta de PHP (8.4.21), facilitando la fase de reconocimiento de un atacante.
[LOW] Configuracion en robots.txt: El archivo bloquea todo el rastreo del sitio y menciona rutas relacionadas con "admin", revelando posibles puntos de interes.